

There are, however, several steps that the Commission should take to help reduce payphone fraud:

(1) On operator-assisted calls from lines equipped with OLS, ICs and operator service providers (OSPs) should be prohibited from allowing such calls to be billed back to the originating station as a direct-dialed call;<sup>23</sup>

(2) In order to prevent regenerated dial tone at payphones, the Commission should amend Section 68.314 of its rules to extend the requirement for delivery of standardized supervisory signals to and from interexchange carriers and OSPs. The rules currently apply only to manufacturers of terminal equipment.

NYNEX certainly agrees that payphone fraud is a serious problem. However, adoption of the Florida PSC rule would unjustifiably relieve payphone providers of their responsibility to utilize other security measures that are available and necessary to combat payphone fraud in addition to LEC BNS and OLS service. The Florida PSC rule would also impose unwarranted liability on the LECs and involve them in continual litigation. The Commission should therefore not adopt the Florida PSC rule.

---

<sup>23</sup> This would also protect private payphone owners (and other call aggregators such as colleges and hospitals) from information providers who accept 800 service calls and subsequently bill these as direct dialed calls despite the OLS restrictions in place.

C. Cellular Fraud

The cellular industry has been working very effectively both within the industry and jointly with law enforcement agencies to combat cellular fraud. However, this process could be enhanced by certain regulatory and legislative actions described below.

1. Revisions to Part 22 of the Commission's Rules

The Commission has proposed a rule (Section 22.929) to help reduce cellular fraud caused by tampering with the ESN. NYNEX supports the rule with several modifications. First, the Commission should require that the ESN chip be secured to the frame of the radio and attached to the logic board by cable. In addition, the software should be encoded and/or scattered over different memory chips. Finally, the rule should also insure that only the original manufacturer's installed ESN is transmitted. This can be accomplished through software and hardware development on the part of the equipment manufacturers. The penalties for failure to meet such requirements should be stiff and enforcement action immediate.

2. Legislative Actions

In conjunction with the proposed Section 22.929 of the Commission's rules, NYNEX recommends that existing laws be modified in such a way as to more clearly place the enforcement of such rules within the jurisdiction of the Secret Service, instead of the Commission. For example, section 1029 of Title 18 of the United States Code should be amended to make it a crime to:

(a) knowingly and with intent to defraud possess a cellular telephone in violation of Section 22.929 of the FCC Rules and Regulations; and

(b) knowingly and with intent to defraud possess a scanning receiver of cellular telecommunication transmissions or hardware and/or software used for altering cellular telephones in violation of 47 U.S.C. 302a(d).

This balanced regulatory and legislative approach will ensure that the Commission is responsible for developing rules and regulations that will reduce fraud and that law enforcement agencies are responsible for ensuring that violators of such rules are properly sanctioned. In this way, the industry, the Commission, and law enforcement officials can work jointly and effectively to solve the cellular fraud problem.

D. LIDB Fraud

As discussed above, NYNEX has taken a number of steps to control calling card, collect and bill to third party fraud. NYNEX has established threshold levels (the number of times a calling card is used within a specified time period) for different classes of customers to help detect and control fraud. When the threshold levels are broken, the LIDB system may automatically deactivate the card so that it can no longer be used. NYNEX's Database Administration Centers operate around the clock to investigate suspected incidents of fraud.

Despite these efforts, calling card fraud cannot be eliminated. As the Commission notes in the NPRM, calling card fraud does not always consist of multiple calls within a short period of time. The fraud might consist of one call of long

duration. There is nothing that the LECs can do to completely stop this type of fraud.

In order to help reduce calling card, collect and bill to third party fraud, the Commission should require ICs, LECs and other telecommunications service providers to validate all calling card, collect and bill to third party calls in LIDB and not complete any calls where positive validation from LIDB is not received. The Commission should also require interexchange carriers to provide LECs with both the calling number and the called number when querying the LIDB database.<sup>24</sup> If this information was provided on calling card, collect and bill to third party calls, the LECs would be better able to use the fraud detection capabilities in their LIDB fraud detection systems to identify areas associated with fraud problems and to develop customer calling pattern profiles that could be accessed to detect suspected fraud.<sup>25</sup>

In addition, carriers can help control fraud on collect and bill to third party calls by refusing to process certain call types that are invariably fraudulent, e.g., coin-originated international calls billed to other domestic numbers. The Toll Fraud Prevention Committee recently adopted

---

<sup>24</sup> The Commission is currently considering the issue of requiring ICs to deliver calling party number to terminating LECs in another proceeding. However, it should be emphasized here that provision of this information can be an extremely valuable tool in preventing toll fraud.

<sup>25</sup> For example, if the LECs were provided with the calling number, they would be able to detect fraud on simultaneous bill to third party or calling card calls originating from distant geographical areas.

a resolution which suggested that long-distance carriers either not process these calls or require the caller to use an alternate billing mechanism such as a calling card or credit card. The Commission should order carriers to utilize one or the other of these two procedures.

E. Subscription Fraud

In the NPRM, the Commission mentions subscription fraud as one of the types of fraud plaguing the cellular industry. It is important to note that subscription fraud is a serious problem with the wireline carriers as well and has been addressed by the Toll Fraud Prevention Committee.<sup>26</sup>

Subscription fraud occurs when a customer subscribes to a telephone service with fraudulent information or false identification and with no intention to pay for the service. Because of their universal service obligations, LECs are compelled to provide service to virtually any applicant.<sup>27</sup> However, state regulations may prohibit LECs from requiring positive identification from applicants. For example, in Maine, NYNEX cannot request photo identification as part of a new service application. In addition, regulations often inhibit LECs from disconnecting, on a timely basis, the service

---

<sup>26</sup> See Attachment C hereto.

<sup>27</sup> On the other hand, interexchange carriers are not required to extend virtually unlimited credit to their customers. In order to help control fraud, the Commission should require ICs to monitor usage on their networks and to develop guidelines for limiting credit on interstate and international calls. When fraud is suspected, ICs should be required to block access to their network.

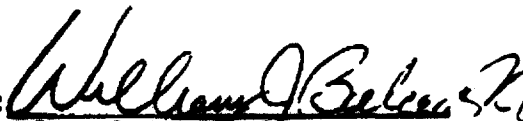
of those persons believed to be engaged in subscription fraud. In addition, state regulations often prohibit LECs from divulging certain customer data to interexchange carriers even when fraud is suspected. The Commission should consider establishing uniform guidelines in all these areas. In order to stop subscription fraud, LECs must be allowed to disconnect service promptly.

V. CONCLUSION

NYNEX will continue its efforts to combat toll fraud. However, the Commission must realize that, despite the most diligent efforts of all parties, toll fraud cannot be eliminated. NYNEX believes that many of the proposals set forth in the NPRM will help reduce toll fraud. However, NYNEX does not support the Commission's proposal to expand liability for toll fraud beyond the limits specified in NYNEX's tariffs. Instead of attempting to develop rules for deciding who is liable for what kind of fraud under which circumstances, the Commission should devote its resources to working with the industry to develop solutions to prevent toll fraud.

Respectfully submitted,

NYNEX Corporation

By:   
Edward R. Whoyl  
William J. Balcerski

120 Bloomingdale Road  
White Plains, NY 10603  
914/644-2032  
Its Attorneys

Dated: January 14, 1994

**A Cooperative Solution to the Fraud that Targets  
Telecom Systems**

**A Position Paper Developed by the  
Toll Fraud Prevention Committee  
of the  
Network Operations Forum**

**Sponsored by the Alliance for Telecommunications Industry Solutions**

**1200 G Street, NW  
Suite 500  
Washington, DC 20005  
(202) 434-8837**

**January 1994**

The Toll Fraud Prevention Committee of the Alliance for Telecommunications Industry Solutions (formerly the Exchange Carrier Standards Association) has reviewed the problem of remote access fraud at private branch exchanges (PBXs), voice mail systems, and other customer premise equipment (CPE). Such fraud is a serious liability for business customers (and other customers) of telecommunications services, resulting in hundreds of millions of dollars of losses annually. To date, no one can say with any confidence that a solution has been found, or that the problem is under control.

Remote access fraud involves the penetration of a PBX or other CPE by one or more unauthorized callers, typically for the purpose of gaining access to restricted information or to network facilities where the defrauder cannot be charged for resulting calls. PBX remote access fraud is frequently used for "call sell" operations, where people pay defrauders to place unlimited calls to international destinations. Compromised access codes (800 or local numbers which reach Direct Inward System Access [DISA] ports and maintenance ports in the PBXs) have a commercial value of thousands of dollars in the toll fraud underworld. Criminals have a significant incentive, consequently, to penetrate telecommunications equipment for remote access fraud.

In analyzing this problem the TFFC determined that there are many actual or potential participants involved in providing CPE of every type to telecommunications users. It is reasonable to expect that each party will act responsibly when providing such equipment, to ensure that appropriate security against remote access fraud is included. The TFFC identified the following as industry segments that are involved in this issue:

- |  |                             |
|--|-----------------------------|
| • the business owner                           | • local telephone companies |
| • the consultant                               | • long distance carriers    |
| • sales & installation firms                   | • law enforcement agencies  |
| • original equipment manufacturers             | • legislators               |
| • manufacturers of adjunct equipment           | • insurers                  |
| • marketers of secondary/refurbished equipment | • consumer/user groups.     |

Many of these segments may be involved in an individual CPE configuration. The typical PBX goes through many steps: a needs assessment, equipment evaluation, purchase decision, equipment design, installation and testing, maintenance, ongoing use, and eventual retirement/replacement. Thus, it falls to many parties to evaluate the security of a telecommunications environment at progressive steps in the equipment's life cycle.

With this distribution of responsibility, security is often neglected. This simplifies enormously the task of defrauders, who persistently look for CPE with lax security to use for their illegal purposes. It is necessary to stress that the business owner, the owner or lessee of the CPE, has the primary and paramount care, custody, and control of the CPE.



The owner has the responsibility to protect this asset, the telecommunications system, equally as well as other financial assets of the business. The PBX is vital to the business's health, since virtually every business survives and thrives by communicating with other businesses and customers. Abuse of the PBX by hackers, even to the disruption of its functioning, can carry a significant financial and operational penalty. Consequently, the business owner must assure that the PBX (and the entire telecommunications environment under the owner's control) is secure from penetration and abuse.

It is worth noting that this form of telecommunications fraud is a crime. Businesses, whether small firms or large corporations, are persons before the law. They also enjoy the same protections as other citizens, including protection from unlawful disruption of their operations and from theft. Therefore, defrauders of these corporate citizens should be prosecuted to the full extent of the law.

It is essential, therefore, that every industry segment support the integration of security into PBXs, voice mail systems, and other CPE. Some segments have a direct role, as is the case for the equipment manufacturer and the installation firm. Others, such as legislators and regulators, have a less direct, but still important role in the control of toll fraud in general, and remote access fraud in particular. The attachment to this position paper outlines the recommendations of the TFFC for each segment of the industry. For each there is a minimal requirement for preventive action, supported by additional steps that each party should take. These recommendations are not exhaustive of all preventive steps, nor will those that are adopted end remote access fraud. However, they will reduce the risks that industry currently faces.

In the judgment of the TFFC, coordination and cooperation are essential to achieving greater success in this area. Consequently, the TFFC urges each industry segment to deliver the maximum protection that it can identify, in supporting customers of telecommunications services.

## **ATTACHMENT: SUGGESTED ANTI-FRAUD EFFORTS BY INDUSTRY SEGMENT**

### **RESPONSIBILITIES OF THE BUSINESS OWNER:**

The basic responsibility of the business owner is to devote adequate resources (time, talent, capital, etc.) to the selection of CPE and to its management, including fraud prevention, detection, and deterrence. It is an essential part of managing the business. The owner must demand that internal staff and supporting external professionals, such as consultants, include security concerns in the evaluation, design and operation of the telecommunication environment for his/her business.

Other efforts are highly recommended to assure that security matches the importance placed on efficiency, economy, accountability, etc., as considerations in PBX and CPE design.

- Enlist knowledgeable professional support (consultants, security experts) as needed.
- Include security as a prime consideration in the definition of system and user needs.
- Require suppliers to provide only the capabilities required/requested. Other features should be made known, with controls, restrictions, vulnerabilities clearly noted.
- Include security support in maintenance agreements. Identify emergency telephone numbers to be used on discovery or suspicion of fraudulent abuse.
- Define and implement an anti-fraud plan. Enlist employees in the plan; provide a feedback system for emergency alerts. Monitor and refine the plan.
- Manage the telecommunications system when installed: monitor usage continually; assign and encrypt passwords; restrict access in, out, and between interconnected nodes of the system; assure the compatibility and security of interconnected CPE.
- Enlist law enforcement agencies when victimized; preserve evidence for prosecution.
- Secure relevant documentation, to avoid compromise and piracy of data, passwords, etc.
- Secure access to the physical facilities, cabling, access ports, administrative terminals, etc.

### **RESPONSIBILITIES OF THE CONSULTANT:**

The consultant supports the business owner in deciding what type of equipment to buy, what type of services to install, and how to configure both equipment and services for

the desired operational environment. It is the consultant's responsibility frequently to act in place of the owner. Consequently, the consultant has the same tasks as the owner. Trained for special expertise, the consultant must place high among his/her priorities the establishment of a secure telecommunications environment. This requires that the consultant be very aware of any fraud implications regarding the system being recommended, and ensure that others involved (vendors, installation technicians, etc.) meet or exceed the levels of security needed. The consultant should take steps to ensure that security is cared at the time of installation and into the future.

Additional support efforts are appropriate:

- Understand all current fraud exposures with CPE, and know how to minimize, if not prevent, exposure in the current telecommunications environment.
- Consider security features when making a recommendation on equipment, and detail in writing to the owner the fraud exposure of the final configuration.
- Understand how features in the local and long distance carrier's services can be used to enhance the security of the equipment.
- Be knowledgeable of and make the owner aware of adjunct equipment that can help prevent and identify abuse.

#### RESPONSIBILITIES OF THE SALES AND INSTALLATION FIRMS:

The sales and installation firms, which will frequently provide ongoing service and maintenance of the CPE, should assist in educating the business owner about the risks and vulnerabilities of the equipment. While stressing the value of the system's features, the sales agents should make known the dangers of toll fraud.

Additional support efforts are appropriate:

- Be completely familiar with the system's features, including those subject to compromise and abuse, such as DISA, maintenance ports, least cost routing features, etc.
- Identify and change any default codes that control access to features and facilities that are subject to compromise and abuse. Secure such replacement codes with responsible management personnel.
- Deactivate features that are not needed, with the full knowledge of the customer.
- Establish time of day restrictions, such as no access to international calling at night and on weekends.
- Restrict access to facilities (WATS, public network "dial 9") and establish calling privileges/limits (internal, local, domestic, international) as appropriate.

## **RESPONSIBILITIES OF THE MANUFACTURERS OF ORIGINAL AND ADJUNCT EQUIPMENT AND THE MARKETERS OF SECONDARY/ REFURBISHED EQUIPMENT:**

These industry segments play a special role in protecting the industry from toll fraud. These manufacturers must develop and deploy flexible and effective security protections to complement the advanced telecommunications features required by businesses. In many cases customers are not aware of the need for such protections and do not request them. They are often unaware of the vulnerabilities of an unprotected system and of the dogged drive of the hacker to find new PBXs to abuse.

Additional support efforts are appropriate:

- List in writing for the customer the features and treatments that are necessary to protect against PBX compromise and abuse.
- Ship only those features that the customer requests; remove default passwords from features such as DISA, so that hackers cannot easily access them.
- Secure in writing that the customer is aware of the system's capabilities and protections.
- Provide emergency contact numbers for customers to use in cases of compromise and abuse.
- Make upgrades to the CPE's controlling software by methods more secure than a dial-up modem with default passwords. For example, update the customer's CPE through call back modems or secure token access devices.
- Care for the security and compatibility of adjunct and refurbished equipment with other interconnected segments of the customer's network.
- Educate the customer thoroughly, including support for user groups, etc.

## **RESPONSIBILITIES OF THE LOCAL TELEPHONE COMPANIES:**

The local telephone companies (LECs) have a supporting role for customers who choose their own PBX and CPE. The LECs may frequently not know what a customer is planning. Nor are the LECs familiar with the wide variety of terminal equipment that is available to business owners. However, they can help to combat fraud by promoting an heightened security concern among all their customers.

Other suggested efforts include:

- Conduct wide customer education through bill inserts, addressing end user groups, holding training seminars, etc.
- Evaluate permitted teaming efforts with long distance companies, equipment manufacturers, etc. to educate customers.
- Evaluate all LEC products and services for security concerns before deployment.

- Where tariffed telecommunications systems are offered, fulfill the above suggested security functions of manufacturer and consultant, as appropriate.
- Alert their customer contact personnel (business office, repair, sales/service) to the signs of toll fraud, so that these staffs can better support business owners who are victimized.
- Deploy network blocking services (such as International Direct Dial Blocking) and call screening information digits to complement customer equipment restriction strategies and long distance company network monitoring.
- Develop network monitoring capabilities to highlight potential fraud patterns (local hacking, 800, international, etc.) as early as possible.
- Expand centralized fraud bureau support to a seven day/24 hour basis.
- Continue the use of security staffs to support long distance company investigations and customer inquiries.
- Cooperate with law enforcement agencies in education, investigation, and prosecution efforts.
- Develop case documentation for federal and local regulators, in support of guidelines allowing timely and responsive security efforts in cases of toll fraud.

#### **RESPONSIBILITIES OF THE LONG DISTANCE COMPANIES:**

The long distance companies (IXCs) are frequently the networks that bear the brunt of toll fraud, because fraudulent calls are often directed to international destinations. IXCs assist in protecting their customers with a variety of monitoring capabilities and protection (indemnity) plans. IXCs also can combat fraud by continuing the extensive educational campaigns to all customers.

Other suggested efforts include:

- Perform network monitoring of 800 calling and calls directed to international destinations, to identify suspected fraud patterns.
- Alert their customer contact personnel (business office, operator services, repair, sales/service) to the signs of toll fraud, so that these staffs can better support business owners who are victimized.
- Include in their network sales efforts educational security information that will alert customers to network vulnerabilities and suggest effective protections.
- Continue the use of security staffs to support customer inquiries.
- Cooperate with law enforcement agencies in education, investigation, and prosecution efforts.
- Develop case documentation for federal and local regulators, in support of guidelines allowing timely and responsive security efforts in cases of toll fraud.

## RESPONSIBILITIES OF REGULATORS:

Regulators perform a critical task in defining how the market acts and reacts. In the case of toll fraud, regulators should recognize that it costs the telecommunications industry (and ultimately consumers and shareholders) billions of dollars annually. Those best able to combat fraud should be empowered to take timely and effective steps to minimize its incidence and severity. In some cases regulatory guidelines might appear to prevent LECs and/or EXCs from disconnecting defrauders in a timely manner. Companies that operate across many states are frequently subject to conflicting rules that do not reflect the realities of systematic, professional toll fraud. Confusion over rules covering collection and security activities allows defrauders to stay on the network. Regulators should act to clarify such areas.

Additional suggestions are:

- Cooperate across jurisdictions (e.g., through NARUC, the FCC) to standardize regulations that allow timely and effective responses against toll fraud.
- Alert customers through periodic press releases about the vulnerabilities of toll fraud and their responsibilities to take effective precautions.
- Stimulate effective legislation punishing toll fraud, and promote its enforcement.
- Allow LECs to deny service, both before it is established and after installation takes place, when warranted by suspected fraud.
- Allow telecommunications service providers to cooperate in combating toll fraud through the exchange of customer information.

## RESPONSIBILITIES OF LEGISLATORS:

Legislators help create the telecommunications environment in response to the drive of technology and market forces. It is essential that they foster a legislative environment in which telecommunications service providers can bring their full skills to the prevention, detection, and deterrence of toll fraud, recognizing that toll fraud is a professional endeavor that continually adapts.

Other steps are:

- Create no anti-fraud mandates that pit segments of the industry against each other, or that allow one segment to avoid responsibility for contributing to the solution.
- Create incentives for the industry to work cooperatively against the problem.
- Support and finance the efforts of law enforcement organizations, so that they are empowered to pursue and prosecute perpetrators of toll fraud.
- Amend the penal codes to remove the relative impunity enjoyed by those who engage in toll fraud as a profession.

### **RESPONSIBILITIES OF INSURERS:**

Insurers can expand the attention that toll fraud receives by including coverage for toll fraud liability in their product portfolios. Insurers can contribute greatly to the education of business customers by discussing risks and protections related to toll fraud, together or separately with other risk coverage that virtually all businesses consider. Packaging and pricing toll fraud liability coverage affordably (yet profitably) will prompt businesses to take effective precautions. This, in turn, will reduce the incidence of remote access fraud.

### **RESPONSIBILITIES OF END USER GROUPS:**

Trade associations and telecommunications end user groups can also broadcast that toll fraud is a significant risk for businesses. Education from many sides will reinforce the necessity for protective action. User groups are particularly valuable in this mode. Frequently, they are aligned by their use of a single technology or a single vendor. Consequently, they can readily share both negative experiences and effective remedies. These groups can also provide the "critical mass" needed to stimulate development of new technology.

### **RESPONSIBILITIES OF LAW ENFORCEMENT AGENCIES:**

While toll fraud might appear as a victimless crime, or one of less pressing priority for prosecution, nevertheless, the operational and financial harm done to businesses by telecommunications defrauders is substantial. Federal and state laws variously define telecommunications fraud and place enforcement responsibilities in many organizations. It is important that this distribution not hinder timely investigations and effective enforcement. Police officers should cooperate across jurisdictions to investigate suspected cases, and district attorneys should prosecute cases to deter future toll fraud and gain restitution for victimized businesses. The enforcement community can also aid the essential educational effort through its own support of end user groups, business councils, etc.

ATTACHMENT B

TESTIMONY OF DIANE GIACALONE

GENERAL MANAGER, SECURITY

NEW YORK TELEPHONE COMPANY

BEFORE THE

HOUSE ENERGY & COMMERCE COMMITTEE

SUBCOMMITTEE ON TELECOMMUNICATIONS AND FINANCE

JUNE 11, 1992



TESTIMONY OF DIANE GIACALONE  
GENERAL MANAGER, SECURITY  
NEW YORK TELEPHONE COMPANY

BEFORE THE

HOUSE ENERGY & COMMERCE COMMITTEE  
SUBCOMMITTEE ON TELECOMMUNICATIONS AND FINANCE

JUNE 11, 1992

I. General introduction

My name is Diane F. Giacalone. I joined New York Telephone Company in February, 1991, and have been its General Manager of Security since July 1991. I was an Assistant United States Attorney in the Eastern District of New York from 1979 to 1988, and have also served as a Trial Attorney in the Tax Division of the Department of Justice. From 1988 to 1991 I was at the Metropolitan Transportation Authority in New York City directing a group that investigated fraud and misconduct.

Mr. Chairman, New York Telephone Company is pleased to have the opportunity to describe our perspective on PEX toll fraud and to outline our role in addressing this problem. After reviewing the PEX toll fraud issue I have concluded that the best defense against this crime is an educated PEX customer working with vendors, long distance and local exchange carriers. All segments of the industry have a role in this process.

My testimony provides some general information on PEX toll fraud from a local exchange carrier perspective, describes our capabilities for monitoring the network, outlines the NYT Security Department's role in PEX toll fraud cases and finally details specific steps that the PEX customer can undertake to prevent or minimize exposure to PEX fraud.

## II. Relationship of PBX to the Public Switched Network

The nationwide telephone network contains a series of discrete components provided by local exchange carriers (LECs), interexchange carriers (IXCs), cellular carriers, and competitive access providers.<sup>1</sup> Customer Premises Equipment (CPE), like the Private Branch Exchange (PBX), while not part of the traditional public communications network, is a critical component of the telecommunications system.

There are several ways telephone traffic is delivered into and out of the PBX. Direct Inward Dialing Trunks (DID), regular inward business lines (IMB), private lines and 800 (inbound WATS) services provide incoming service. Calls are routed out of the PBX onto outgoing trunks, WATS lines, private lines and tie lines to other PBX facilities. Incoming and outgoing services are generally provided by local exchange carriers, but they may be carried by IXCs, or competitive access providers, bypassing the local exchange carrier.

## III. PBX Fraud

Many Private Branch Exchanges contain a feature called remote call access or Direct Inward Switched Access (DISA). This feature permits individuals outside a business location to place long distance calls through the PBX. The PBX owner is billed for the call.

Remote access to the PBX is gained by dialing a local or 800 number for the PBX. Once inside the PBX, the caller may then use the PBX for outbound calls. Most PBXs are programmed to require use of an internal Personal Identification Number (PIN) to prevent unauthorized access to the outbound lines.

---

1     E.g., Metropolitan Fiber Systems, Inc., Teleport Communications Group.

PBX fraud occurs when someone gains unauthorized access to the outbound lines. Most often, an intruder calls into the PBX via an 800 number and attacks the PIN protection. This can be done by use of a computer program that continues to redial the PBX until a valid PIN is found. Once a valid PIN is known, that PIN can be used to fraudulently gain access to outbound long-distance lines.<sup>2</sup>

#### IV. LEC Role in delivering calls to and from PBXs

A local exchange carrier's role is confined to the portion of the communications activities that occur on LEC facilities outside of the PBX. We usually provide the last link in the public switched network for incoming calls destined for a PBX and the corresponding first segment of the route for outgoing calls. Because of that circumscribed role, the information that we receive is very limited. The amount of information that can be gathered, collated and analyzed by the long distance carrier and by the PBX customer is much greater than that in possession of the LEC.

The local exchange carrier receives limited information about calls coming into a PBX. The major risk at present for PBX fraud involves use of 800 service to place calls to a PBX using the PBX remote access feature. In most instances, a call placed to an interexchange 800 number is directed by the local exchange carrier to the appropriate IXC. Typically, the IXC translates the 800 number into a 10-digit (1+ area code + local 7 digit ) number.

---

2 NYT provides a remote access feature associated with its Centrex-service (known as Intellipath) services as an optional service. It is not activated without customer approval. In addition, INTELLIPATH customers can purchase customer premise equipment, through which they provide and administer the remote access feature. NYT would have no knowledge or involvement with the remote access operations of these latter customers. NYT does not provide the administration of the Remote Access feature for its Centrex customers.

Thus 800 calls delivered by an IXC are indistinguishable from normally dialed 10-digit interstate calls or calls coming from another local telephone location. To the local exchange carrier, all incoming 10 digit calls look exactly the same.

Similarly, the local carrier has limited information about the calls leaving the PEX. When the local company provides the outbound service, the called number is transmitted to the local network because that is the only information necessary for the local carrier to fulfill its role — to deliver the call to a terminating intralATA destination or to an interexchange carrier if it is an interLATA call (typically interstate or international).<sup>3</sup>

Normally, the local carrier knows nothing about the ultimate destination of a call that has been delivered to the PEX. Because the PEX itself transfers a remote access 800 call from an inbound call to an outbound call, the local carrier can not link the incoming and outgoing calls in order to discern suspicious activity.

The local carrier, therefore, delivers and receives individual calls from PBXs and other customer premises equipment but normally sees no specific characteristics that distinguish legitimate from illegitimate use. Only detailed analysis of length of call, countries called, number of attempts per hour, etc., will disclose possible fraudulent or illegitimate use.

---

<sup>3</sup> The consent decree, the Modification of Final Judgment (MFJ) that divested the local Bell Operating Companies (BOC) from AT&T, created LATAs (Local Access Transport Areas). BOCs may only transmit end-to-end calls within these areas (intralATA calls); calls between LATAs (interLATA calls) must be carried by interexchange carriers. Under the MFJ, NYT is obligated to hand off interLATA (predominantly interstate) and international calls to the end user's designated interexchange carrier without discrimination.

V. LEC Analysis of Calling Activity

NYT monitors its network in various ways, ranging from general network traffic surveillance to the scrutiny of specific calls including digits dialed, frequency, and length of call. The reasons for monitoring range from concern with the efficiency of transmission and completion of calls to detection of fraudulent conduct.

a) General Network Monitoring

General network monitoring is controlled by NYT's Network Service Center. This engineering function is designed to provide network management of NYT's primary responsibility -- the successful, completed transmission of telephone calls. The Network Service Center examines network parameters to pinpoint overloaded trunks and overloaded switches. Call completion data are analyzed to determine whether calls are not complete because of busy signals or no answers or due to network failures.

These activities are designed to give early indications of potential network failure or blockage. They are not intended to, nor are they effective at, detecting instances of fraud.

Despite the general unsuitability of this technique for fraud detection, from time to time episodes of PBX fraud are identified. When the Network Service Center identifies blocked (i.e., over-loaded) incoming PBX trunk routes, customers often are contacted to try to determine and eliminate the cause of the problem. Most often, the overloaded trunks are directly related to the customer's legitimate business call volumes. However, twice in the past six months, NYT customers have confirmed that PBX fraud was the cause of the blocked trunks.

It is critical to understand that this type of network monitoring is done on an aggregate basis. Individual customer calling patterns are not

scrutinized. In addition, this technique can only identify PBX toll fraud when the symptom is blocked DID trunks. In many instances the PBX capacity is such that the fraud is likely to occur without any blockage or overloading of the PBX trunks.

b) Bill Detail Monitoring

Another method of monitoring uses billing details to monitor customer calling patterns. Bill detail monitoring is not done on a real time basis, and can only be done where NYT bills for the calls.<sup>4</sup>

One internal billing alert mechanism used by NYT is the High Toll Notifier. Using thresholds and criteria set by New York Telephone with interexchange carrier knowledge, NYT examines carrier provided bill details for those carriers for whom we provide billing and collection services. This procedure alerts the business office to particularly high usage over a short interval in the billing cycle. It enables a Service Representative to evaluate further extensions of credit for calls and also to alert the business or residence customer or the IXC that unusual usage is developing on the line or that usage exceeds acceptable pre-determined levels for that customer.

The High Toll Notifier analysis is performed toward the end of the billing cycle, and therefore the High Toll Notifier alert provides only after-the-fact information to NYT's business offices. It is used to limit uncollectibles, not to detect fraud.

In December 1991, NYT Security was instrumental in introducing a trial of a new fraud detection tool, the Advance Toll Notifier. NYT Security, interexchange carriers, Business Office Managers and law enforcement officials

---

<sup>4</sup> NYT bills for its intralATA calls and services provided by NYT. NYT also offers a billing service to IXCs. When NYT acts as the billing agent for an IXC, there are contracts that govern NYT's responsibility as a billing agent.

have developed various criteria that are reliable indicators that a particular line is being used to commit toll fraud. The threshold criteria include: (i) countries to which high volumes of fraud calls are placed, (ii) international calls that use a "Three Way Dialing" feature; and (iii) all lines that generate over a designated dollar value in international volume during a one to three day cycle. These criteria are used to analyse NYT's internal Automatic Message Accounting (AMA) tapes that contain information about all calls that were made on the local network.

The Advance Toll Notifier reports are generated within 3 days of the actual call date, well in advance of billing dates but still after fraud has occurred. The reports are examined by Business Office representatives, who call customers when high volume of transactions exceeding the thresholds are identified.

Although the Advance Toll Notifier is not directed specifically at PBX fraud, two instances of PBX fraud have been identified to date.

The Advance Toll Notifier is an analytical tool that uses criteria that are refined as we learn more about each new type of fraudulent activity. The more information available to us, the more precise our criteria, thresholds and analysis. The Advance Toll Notifier, however, is still an after-the-fact technique based upon general fraud patterns. Customers with smart PBXs have the ability to set criteria and thresholds designed specifically to reflect their own operations and calling patterns. Such individually designed tools will be far more efficient and effective than those based on generic criteria.<sup>5</sup>

---

<sup>5</sup> We recognize in this connection that AT&T and Sprint have recently announced services to limit PBX toll fraud and to guarantee the PBX user against loss. These interexchange carriers' programs both educate the PBX user and require the PBX user to take certain protective actions, and then use computer techniques and pre-set criteria and thresholds to analyze calls and to identify and preclude fraudulent calling activities.

c) NYT Security Department Activity

When the NYT Security Department is in possession of specific information about the commission of fraud directly involving NYT's facilities, we attempt to take direct action. The most common source of such fraud for NYT involves the unauthorized use of compromised calling or credit cards and personal identification numbers to make long distance calls from public telephones. As we identify specific public telephone locations that are the sites of significant fraudulent activities, we install or activate devices to record information about calls made from those phones, including the personal identification numbers and calling card numbers used, terminating telephone numbers, and length of call. Using length of calls as a screening device, the terminating numbers and PINs are analyzed to identify unauthorized uses of credit cards. If considered compromised, the calling cards issued by NYT are then disabled. We inform interexchange carriers when their calling cards appear to be misused and they are able to take appropriate action.

Until recently, this analysis was done manually and was very labor intensive. At present we are testing software applications that use new devices in public coin operated telephones to collect, store, sort and analyze this data more quickly and efficiently. Despite this increased capability, analysis remains cumbersome, and we are limited both by resources and sheer volume of the information we receive that may involve fraudulent activity. At present we can monitor only a very few of the many public telephone lines in service.

NYT Security is not now investigating any instances of PBX fraud. On occasion we assist long distance carriers in their investigations of PBX fraud by installing dial number recorders to lines showing strong indications



of use for fraud.<sup>6</sup> In addition, we assist PBX owners who discover that they have been the victims of unauthorized intrusion by advising them: (1) to disable their remote access features immediately; (2) to institute stricter security measures before enabling the remote access feature again; and, (3) to call the manufacturer or vendor of the equipment for assistance in instituting stricter security measures.

VI. Educating PBX Users About Remote Access PBX Toll Fraud

The best approach to the prevention of PBX fraud is the the education of the PBX owner. NYT Security has designed an instruction package that describes the nature and source of PBX abuse, some of the early symptoms of intrusion, and techniques that a PBX owner may use to prevent being victimized. The program is being presented to NYT employees who have contact with PBX owners. Those employees will be able to raise with PBX users the issues of vulnerability and protection that are so important to the owner of a PBX.

In our instruction package we emphasize that PBX users have a range of options both to prevent remote access fraud and to detect it promptly if it occurs. The PBX vendor is the best source of information about the specific features available on each PBX.

Once aware of the security and analysis options available on the PBX, the PBX owner can devise effective screening and alert mechanisms using its extensive and detailed information about normal usage patterns for its business in combination with information about general patterns that are

---

<sup>6</sup> NYT is rarely asked to assist in these PBX fraud cases, because once fraud is identified, the PBX customer and IRC generally have all the information they need to investigate the crime.